(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2000-0012131
H04L 29/06		(43) 공개일자	2000년02월25일
(21) 출원번호	10-1999-0031537		
(22) 출원일자	1999년07월31일		
(30) 우선권주장	9/127,769 1998년07월31일 미국(US)		
---	---
(71) 출원인	루센트 테크놀러지스 인크 미국 000-000 미합중국 뉴저지 머레이 힐 마운틴 애비뉴 600 (우편번호 : 07974-0636)
(72) 발명자	베렌즈웨이그아담엘. 미국 미국,뉴욕1003,뉴욕,이스트12번가스트리트70 파텔사바 미국 미국,뉴져지07045,몬트빌,밀러레인34
(74) 대리인	이병호
(77) 심사청구	없음

(54) 출원명 공중 전파 통신과 패스워드 프로토콜을 사용하여 키를 확립하는 방법 및 패스워드 프로토콜

요약

패스워드 프로토콜에 있어서, 통신 파티(party) 들은 각각이 지수 함수를 포함하는 계산 결과를 교환하여 키를 발생한다. 계산 결과의 발생에 있어서, 각 파티는 그들의 각 지수 함수에 패스워드를 추가한다. 한 파티에 의해 미리 전송되는 인증 정보가 다른 파티에 의해 승인되면, 상기 다른 파티는 패스워드 프로토콜에 따라 확립된 키를 사용한다. 채널 인증 정보는 통신 보안 채널을 통해 전송된다. 이 통신 보안 채널은 또한 상기 파티들간에 전송되는 적어도 1개의 계산 결과 상의 해시를 검증하기 위해 다른 실시예에서 사용되기도 한다. 해시가 검증되면, 상기 파티 들간에 전송된 계산 결과를 사용하여 키를 확립한다.

대표도

도3

색인어

인증 정보, 세션 키, 통신 보안 채널

명세서

도면의 간단한 설명

도 1은 디프-헬만 키 규약(Diffe-Hellman key agreement)에 의한 네트워크와 모빌 간의 통신을 도시하는 도면.

도 2는 디프-헬만 암호화 키 교환 프로토콜에 따른 네트워크와 모빌 간의 통신을 도시하는 도면.

도 3은 본 발명의 실시예 1에 의한 전화 회선/지상 통신선 및 모빌을 통한 네트워크와 모빌 유저간의 통신을 도시하는 도면.

도 4는 본 발명의 실시예 2에 의한 전화 회선/지상 통신선 및 모빌을 통한 네트워크와 모빌 유저간의 통신을 도시하는 도면.

도 5는 본 발명에 실시예 3에 의한 전화 회선/지상 통신선 및 모빌을 통한 네트워크와 모빌 유저간의 통신을 도시하는 도면.

도면의 주요부분에 대한 부호의 설명

10 : 네트워크 30 : 전화 회선/지상 통신선

20 : 모빌

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 패스워드 프로토콜과 공중 전파 통신을 사용하여 키를 확립하기 위한 방법에 관한 것이며 일실시예는 패스워드 프로토콜에 관한 것이다.

무선 통신 시스템에서, 흔히 모빌이라 불리며 모빌 유저가 구입하는 핸드세트는 전형적인 경우에 네트워크 서비스 프로바이더에 가입되고, 이 핸드 세트에는 롱 키(long key)와 파라미터가 서비스의 실행을 위해 기입된다. 서비스 프로바이더의 네트워크는 또한 모빌과 관련하여 관련 모빌에 대한 롱 키와 파라미터의 카피를 보유하고 있다. 주지되어 있는 바와같이, 정보는, 이들 롱 키와 파라미터에 기초하여, 네트워크와 모빌 간에 공중 전파를 통해 전달될 수 있다.

대안적으로, 유저는 서비스 프로바이더로부터 전화 회선/지상 통신선 등의 통신 보안 채널을 통해 롱 키를 수신하고 이들 코드를 수조작으로 모빌에 입력할 필요가 있다.

롱 키와 파라미터의 전달은, 공중 전파에 대조되는 전화 회선/지상 통신선을 통해 네트워크 서비스 프로바이더에서 실행되기 때문에, 공중 침입에 대해 안전하다. 그러나, 이러한 정보의 안전한 전달 방법은 어떤 의무와 규제를 모빌 유저에게 부과하고 있다. 양호하게, 모빌 유저가 그들의 핸드세트를 구입하게 되면, 서비스 프로바이더의 장소에 핸드세트를 실제 가져가거나 어떤 오류도 없이 모빌에 롱 키를 수조작으로 입력하지 않아도, 어떤 서비스 프로바이더로부터 서비스를 받게 된다. 모빌을 원격으로 가동시키기 위한 기능은, 북 아메리카의 무선 통신 규격에 규정되어 있으며, "over the air service provisioning"(OTASP)으로 참조되고 있다.

현재, 북 아메리카의 셀룰러 규격(IS41-C)은 쌍방 간에 보안 키를 확립하기 위한 주지의 디프 헬만 키 규약(Difee-Hellman(DH) key agreement)를 사용하는 OTASP 프로토콜을 정의하고 있다. 도 1은 IS41-C에 사용되는 모빌(20)과 네트워크(10) 간의 보안 키 확립에 대한 DH 키 규약의 애플리케이션을 설명한다. 즉, 도 1은, 명료함을 위해, DH 키 규약에 따른 네트워크(10)와 모빌(20) 간의 통신을 단순한 형태로 도시하고 있다. 본 명세서에 사용되는 바와같은, 네트워크라 함은, 서비스 프로바이더에 의해 동작되는 인증 센터, 홈 위치 레지스터, 방문 위치 레지스터, 모빌 스위칭 센터, 및 네트워크 기지국에 관련되어 있다.

네트워크(10)는 난수(R_N)를 발생하고 ($g^{R_N} \bmod p$)를 계산한다. 도 1에 도시된 바와같이, 네트워크(10)는 모빌(20)에 512 비트의 소수(p)와, 소수(p)에 의해 발생되는 그룹의 생성원(g), 및 ($g^{R_N} \bmod p$)를 전달한다. 다음에, 모빌(20)은 난수(R_N)를 발생하고 ($g^{R_M} \bmod p$)를 계산함과 함께, 네트워크(10)에 ($g^{R_M} \bmod p$)를 전달한다.

모빌(20)은 네트워크(10)로부터 수신한 ($g^{R_N} \bmod p$)를 R_M 으로 자승하여 ($g^{R_M R_N} \bmod p$)를 구한다. 네트워크(10)는 모빌(20)로부터 수신한 ($g^{R_M} \bmod p$)를 R_N 으로 자승하여 또한 ($g^{R_M R_N} \bmod p$)를 구한다. 모빌(20)과 네트워크(10) 양자는 동일한 결과를 얻게 되고, 64 최하위 비트를 A 키로 불리는 롱 키로서 확립한다. A 키는 모빌(20)과 네트워크(10) 간의 통신 보안을 위해 사용되는 다른 키를 도출하는 루트 키로서 기능한다.

상기 DH 키 교환에서의 문제 중 1가지는, DH 키가 인증되지 않고 앤-인-더-미들(man-in-the-middle) 침입을 당하게 된다는 것이다. 예컨대, 상기 모빌과 네트워크를 2파티로 하는 예에서, 침입자는 네트워크(10)와 네트워크(10)에 대한 모빌(20)로서 번갈아 위장할 수 있다. 이러한 양태에서 침입자는 모빌(20)과 네트워크(10) 간에 메시지를 중계할 때의 A 키를 알고 있고 그것을 선택하여 인증 요건을 충족시킨다. 상기 DH 키 교환은 또한 오프 라인 딕셔너리 침입(off-line dictionary attack)의 가능성도 있다.

A 키 등 공중 전파를 통한 정보의 전달을 보호하기 위한 또다른 주지의 프로토콜로서는, 디프 헬만(Diffe-Hellman) 암호화 키 교환(DH-EKE)이 있다. DH-EKE는, 정보를 교환하기 위한 프로토콜에 기초한 패스워드이며, 공중 전파를 통한 전송 이전에 모빌 사용자와 네트워크 서비스·프로바이더 양자가 패스워드를 확립하고 있다. 도 1에 관하여 설명한 DH 키 교환 시스템과는 달리, DH-EKE는 앤-인-더-미들 침입과 오프라인 딕셔너리 침입을 차단한다.

도 2와 관련하여 DH-EKE를 설명한다. 도 2는 DH-EKE 프로토콜에 의한 모빌(20)과 네트워크(10) 간의 통신을 설명하고 있다. 도시한 바와같이, 모빌(20)은, 512 비트의 소수(p)와 네트워크(10)에 대한 생성원(g)을, 모빌 사용자와 네트워크(10)에 알려져 있는 패스워드(p)를 사용하여 암호화/복호화 알고리즘(ENC)에 따라서 암호화된 ($g^{R_M} \bmod p$)를 암호화 키로서 함께 전달한다. 이러한 계산은 $ENC_p(g^{R_M} \bmod p)$로서 표현된다. 네트워크(10)는 패스워드(P)를 사용하여 ($g^{R_M} \bmod p$)를 복호하고, ($g^{R_M R_N} \bmod p$)와 등가인 $(g^{R_M} \bmod p)^{R_N}$을 계산한다. 네트워크(10)는 ($g^{R_M R_N} \bmod p$)와, 이 값의 해시(hash), 또는 그것의 일부를 세션 키(SK)로서 선택한다.

다음에, 네트워크(10)는 ENC에 따라서 패스워드(P)를 사용하여 암호화된 ($g^{R_N} \bmod p$)와 ENC에 따라서 세션 키(SK)를 사용하여 암호화된 난수(R_N ')를 모빌(20)에 전달한다. 모빌(20)은 패스워드(P)를 사용하여 ($g^{R_N} \bmod p$)를 복호하고, ($g^{R_M R_N} \bmod p$)와 등가인 $(g^{R_N} \bmod p)^{R_M}$을 계산한다. 다음에, 모빌(20)은 ($g^{R_M R_N} \bmod p$)와, 그것의 해시, 또는 그것의 일부를, 네트워크(10)에서 행한 바와같이, 세션 키(SK)로서 선택한다. 다음에, 모빌(20)은, 세션 키(SK)를 사용하여, R_N '를 복호한다.

다음에, 모빌(10)은 난수(R_M ')를 발생하고, ENC 에 따라서 세션 키(SK)를 사용하여 난수(R_M ', R_N ')를 암호화며, 암호화된 난수(R_M ', R_N ')를 네트워크(10)에 전달한다. 네트워크(10)는 난수(R_M ', R_N ')를 세션 키(SK)를 사용하여 복호하고, 또한 R_N '를 복호화한 것이 모빌(20)에 최초로 전송된 R_N '과 등가인 지를 판정한다. 세션 키(SK)는, R_N '를 복호한 것이 모빌(20)에 최초로 전송된 R_N '과 등가인 때 네트워크(10)에 의해 검증된다.

다음에, 네트워크(10)는 ENC 에 따라서 세션 키(SK)를 사용하여 암호화된 난수(R_M ')를 모빌(20)에 전달한다. 모빌(10)은 암호화된 난수(R_M ')를 세션 키(SK)를 사용하여 복호하고, 또한 R_M '를 복호화한 것이 네트워크(10)에 최초로 전송된 R_M '과 등가인 지를 판정한다. 세션 키(SK)는, R_M '를 복호한 것이 네트워크(10)에 최초로 전송된 R_M '과 등가인 때 모빌(20)에 의해 검증된다.

네트워크(10)와 모빌(20)이 세션 키(SK)를 검증하면, 세션 키(SK)는 A 키로서 사용되고, 모빌(20)과 네트워크(10) 간의 통신이 상기 A 키를 사용하여 재구성된다.

발명이 이루고자 하는 기술적 과제

DH-EKE 프로토콜에 의하면, 앤-인-더-미들 침입과 오프-라인 딕셔너리 침입을 차단하지만, 정보가 누출될 우려가 여전히 존재하고, 또한 침입자가 패스워드(p)를 복원할 우려도 있다.

발명의 구성 및 작용

패스워드 프로토콜에 있어서, 통신을 행하는 파티들은 각각이 지수함수를 포함하는 계산 결과를 교환하여 키를 발생하고 있다. 계산 결과의 발생에 있어서, 각 파티들은 그들의 각 지수함수에 패스워드를 추가한다. 한 파티에 의해 미리 전송된 인증 정보가 다른 파티에 의해 승인되면, 상기 다른 파티는 패스워드 프로토콜에 따라 확립된 키를 사용한다. 상기 인증 정보는 통신 보안 채널을 통해 전송된다. 각 지수 함수에 패스워드를 추가함으로써, 패스워드 정보가 누출된 우려가 적어지고 상기 계산이 보다 유효하게 된다.

통신 보안 채널은 또한 파티들간에 전송된 적어도 1개의 계산 결과 상의 해시(hash)를 검증하기 위한 다른 실시예에서도 사용되고 있다. 그러나, 패스워드 프로토콜과는 달리, 상기 계산 결과는 패스워드를 포함하고 있지 않다. 해시가 검증되면, 파티들간에 전송된 계산 결과를 사용하여 키를 확립하게 된다. 이 검증 절차에서는 키를 확립하기 이전에 보안을 위한 절차를 제공하고 있다.

본 발명은 파티(party)로서 모빌 유저와 네트워크를 사용하는 무선 (통신) 산업을 포함하는 각종 분야에 적용된다.

이하에서는 무선 시스템의 응용으로서, 공중 전파 통신을 사용하여 키를 확립하기 위한 본 발명의 시스템 및 방법을 설명한다. 즉, 모빌(20)과 네트워크(10) 간에서 전화 회선/지상 통신선(30)을 통해 키를 확립하는 방법 및 패스워드 프로토콜에 대한 일실시예를 설명한다.

도 3은, 전화 회선/지상 통신선(30) 및 본 발명의 실시예 1에 의한 모빌(20)을 사용하는, 네트워크(1)로서 총칭되는 (1) 네트워크 프로바이더와 네트워크(10)와, (2) 모빌 유저 간의 통신을 설명한다. 도시된 바와같이, 전화 회선/지상 통신선(30)을 통해서, 모빌 유저는 네트워크(10)에 인증 정보(예컨대, 과금(billing)을 위한 신용 카드 정보)를 제공한다. 네트워크(10)가 인증 정보를 승인하면, 네트워크(10)는 전화 회선/지상 통신선(30)을 통해서 모빌 유저에게 4 디지트의 패스워드(P)를 제공한다. 그러나, 패스워드(P)는 4 디지트 이상이거나 그 이하일 수 있다.

다음에, 모빌 유저는 이 짧은 패스워드(P)를 활성 프로그램의 부분으로서 모빌(20)에 입력한다. 모빌(20)은, 난수 발생기를 사용하여, 난수(R_M)를 발생하고, 사전에 기억된 512 비트의 소수(p)와 소수(p)에 의해 발생되는 그룹의 생성원(g)을 사용하여 ((g^R_M +p) mod p)를 계산한다.

모빌(20)은 소수(p)와 생성원(g)을 ((g^R_M +p) mod p)과 함께 네트워크(10)에 전송한다. ((g^R_M +p) mod p)는 ((g^RM mod p)+(p mod p)와 등가이기 때문에 네트워크(10)는 패스워드(P)를 인식하고 (P mod p)와 ((g^R_M mod p)를 ((g^R_M +p) mod p)로부터 계산한다. 난수(R_N)를 발생한 후, 네트워크(10)는 (g^R_M R_N mod p)와 등가인 (g^RM mod p)를 계산한다. 네트워크(10)는 (g^R_M R_N mod p)와, 그것의 해시 또는 그것의 일부를 세션 키(SK)로서 선택한다. 예컨대, IS41 프로토콜를 참조하면, (g^R_M R_N mod p)의 적어도 64 최하위 비트가 세션 키(SK)로서 선택될 것이다.

다음에, 네트워크(10)는 ((g^R_N +p) mod p)를 계산하여 모빌(20)에 전송한다. 모빌(2)은, (g^R_N mod p)를 추출한 후, (g^R_M R_N mod p)와 등가인 (g^R

$_N$ mod p)^R_M를 계산한다. 모빌(20)은, 네트워크(10)에서와 같이, (g^R_M R_N mod p)와, 그것의 해시, 또는 그것의 일부를 세션 키(SK)로서 선택한다. 예컨대, IS41 프로토콜을 참조하면, 세션 키(SK)로서 (g^R_M R_N mod p)의 적어도 64 최하위 비트가 선택될 것이다.

네트워크(10)와 모빌(20)이 세션 키(SK)를 가지게 되면, 세션 키(SK)는 A 키로서 사용되게 되고, 모빌(2)과 네트워크(10) 간의 통신이 상기 A키를 사용하여 재 구성된다.

상술한 본 발명의 공중 전파 교환은 DH-EKE 프로토콜이 정보를 유출하는 정도에 비해 정보를 누출하지 않는 패스워드 프로토콜(즉, 도 3의 ((g^R_M +p) mod p)와 ((g^R_N +p) mod p))을 사용한다. 또한, 이 패스워드 프로토콜은 패스워드의 효과가 상실되도 정보가 누설되는 우려가 없기 때문에 안전한다. R_M 과 R_N 은 일정한 난수이다. 이들 난수를 g로 자승하고 mod p로 감산하면, 누승법 mod p에 의해 유발되는 순열(permutation)로 인하여 일정한 난수가 된다. 그래서, P mod p를 그 수에 추가하면 그 결과의 일정함과 무작위 정도(randomness)가 변하지 않게 되고, 다른 패스워드의 효과가 상실되더라도 적당한 수를 등가적으로 생성하게 되어 정보의 누출을 방지할 수 있다. 당업자라면 상술한 패스워드 프로토콜이 정보의 공중 전파 교환 분야에 국한되는 것은 아님을 알 수 있을 것이다. 예컨대, 이 패스워드 프로토콜은 엔터티(entity) 인증과 세션 키 규약에 적용될 수 있다.

이하에서는 본 발명의 실시예 2를 도 4에 대하여 설명한다. 도 4는 본 발명의 실시예 2에 따른, 전화 회선/지상 통신선(30)과 모빌(20)을 통한 네트워크(10)와 모빌 유저 간의 통신을 도시하고 있다. 도시한 바와같이, 전화 회선/지상 통신선(30)을 통하여, 모빌 유저는 네트워크(10)에 인증 정보를 제공한다. 네트워크(10)가 인증 정보를 승인하면, 모빌(20)은 모빌의 초기 절차 중 일부로서 초기화 요구를 발행하므로, 초기화 절차가 이어지게 된다.

네트워크(10)는 난수(R_N)를 발생하고 모빌(20)에 (g^R_N mod p)를 전송한다.

모빌(20)과 네트워크(10) 양자는 주지의 보안 해싱(Hashing) 알고리즘(SHA)을 사용하여 (g^R_N +p) mod p)와 (g^R_M mod p) 상의 집합적 해시인, h((g^R_N +p) mod p), (g^R_M mod p))를 실행한다. 그러나, 어떤 해싱 알고리즘을 사용할 수 있음을 유의하라. 모빌(20)은 해시의 결과를 표시하고, 모빌 유저는, 전화 회선/지상 통신선(30)을 통해, 해시의 디지트를 네트워크(10)에 전송한다.

네트워크(10)가 모빌 유저에 의해 제공된 디지트와 네트워크(10)에 의해 행해진 해시와의 일치를 확인하면, 통신이 검증되고 A키가 (g^R_M R_N mod p)와 그 해시 또는 그 일부로서 확립되게 된다. 즉, 이렇게 하여 모빌(20)은 A키를 확립하게 되고, 네트워크(10)는 해시가 검증되는 경우 이 A 키를 모빌(20)에만 관련시킬 것이다.

대안적으로 실시예 3은, 모빌 유저(20)는, 모빌(20)과 접촉할 수 있고 (g^R_M +p) mod p)를 초기 통신으로서 전송할 수 있도록, 인증 정보와 함께, 충분한 정보(예컨대, 모빌의 식별 번호 등)를 네트워크(10)에 공급한다.

이 실시예 3은 버스데이 침입(birthday attack)과 관련되어 있다. 즉, 이 프로토콜을 1회 이상 침입해야만 하는 맨-인-더-미들(man-in-the-middle)에 의해 시도되는 침입 중 절반이 최초로 나타나고 있다. 그러나, 실시예 3의 대안적인 예에 의하면, 해시가 h((g^R_M mod p), (g^R_N mod p), (g^R_M R_N mod p))로 변경되는 경우에, 침입자는 해시를 사용하여 누승을 실행하지 않으면 안되기 때문에, 상기 침입이 꽤 지연되게 된다.

실시예 3의 다른 대안적인 예로서는, 모빌(20)과 네트워크(10) 간의 통신을 검증하기 위해 실행되는 해시가, 모빌(20)의 식별 번호를 포함하는 것이 있다.

실시예 3의 또다른 변형예(즉, 본 발명의 실시예 4)에 의하면, 모빌(20)은, 도 4에 도시된 바와같이, 네트워크(10)로부터 (g^R_M mod p)를 수신한 후에야 (g^R_M mod p)를 네트워크(10)에 전송한다. 실시예3에 있어서는, 맨-인-더-미들 침입자가 (g^R_M mod p) 와 (g^R_M

수 있었고, 그에 따라서 버스데이 침입이 조장되었다. 본 실시예 4에 의하면, 침입자는 모빌(20)이 ($g^{R_M} \bmod p$)를 알 $\bmod p$)를 처리하여만 한다. 이것은 침입자의 자유도를 1씩 저감한다.

도 5는 본 발명의 실시예 5에 의한 전화 회선/지상 통신선(30)과 모빌(20)을 통한 네트워크(10)와 모빌 유저간의 통신을 도시한다. 도시된 바와 같이, 모빌 유저는, 전화 회선/지상 통신선(30)을 통해, 네트워크(10)에 인증 정보를 제공한다. 상술한 바와같이, 모빌(20)은, 인증 정보와 함께, 네트워크(10)에 이 네트워크(10)가 모빌(20)과 초기 접촉을 하도록 하는 충분한 정보(예컨대, 모빌 식별자 등)를 공급할 수 있다. 네트워크(10)가 상기 인증 정보를 승인하는 경우에는, 인증 절차가 행해질 것이다.

인증 절차는 다른 파티에 대해 초기화 요구를 전송하는 모빌(20)과 네트워크(10) 중 하나에서 계속적으로 행해진다.

예컨대, 모빌(20)이 초기화 요구를 전송하면, 네트워크(10)는 난수(R_N)를 발생하고, ($g^{R_N} \bmod p$)와 ($g^{R_N} \bmod p$)의 해시를 계산한 후, h($g^{R_N} \bmod p$)를 모빌(20)에 전송한다. 모빌(2)은 난수(R_M)를 발생하고, ($g^{R_M} \bmod p$)를 계산한 후, ($g^{R_N} \bmod p$)를 네트워크(10)에 전송한다. 네트워크(10)는 그것에 응답하여 모빌(20)에 ($g^{R_N} \bmod p$)를 전송한다.

다음에, 모빌(20)은 수신한 ($g^{R_N} \bmod p$)의 해시를 계산하고 이 계산된 h ($g^{R_N} \bmod p$)가 네트워크(10)로부터 초기에 수신한 것과 등가인지를 확인한다. 등가인 것으로 확인되면, 초기화 절차가 계속적으로 행해진다.

즉, 모빌(20)과 네트워크(10) 양자는 h(($g^{R_M} \bmod p$), h($g^{R_N} \bmod p$))를 행한다. 모빌(20)은 해시의 결과를 표시하고, 모빌 유저는, 전화 회선/지상 통신선(30)을 통해서, 해시의 디지트를 네트워크(10)에 전송한다.

네트워크(10)가 상기 디지트가 네트워크(10)에 의해 실행된 해시와 일치한다고 판정하면, 통신이 검증되고 A 키가 ($g^{R_M R_N} \bmod p$)와, 그것의 해시, 또는 그것의 일부로서 확립된다. 즉, 이렇게 하여 모빌(20)은 A키를 확립하게 되고, 네트워크(10)는 해시가 검증되는 경우 모빌(20)에만 상기 A키를 관련시키게 된다.

상술한 바와같이 모빌(20)이 초기화 요구를 전송하지 않고, 네트워크(10)가 초기화 요구를 전송할 수 있다. 네트워크(10)가 초기화 요구를 전송하면, 모빌(20)은 난수(R_M)를 발생하고, ($g^{R_M} \bmod p$)와 ($g^{R_M} \bmod p$)의 해시를 계산한 후, h($g^{R_M} \bmod p$)를 네트워크(10)에 전송한다. 그것에 회답하여, 네트워크(10)는 난수(R_N)를 발생하고, ($g^{R_N} \bmod p$)를 계산하여 ($g^{R_N} \bmod p$)를 모빌(20)에 전송한다. 그것에 회답하여, 네트워크(10)는 모빌(20)에 ($g^{R_N} \bmod p$)를 전송한다.

다음에, 모빌(20)이 수신한 ($g^{R_N} \bmod p$)의 해시를 계산하고 이 계산된 h ($g^{R_N} \bmod p$)가 네트워크(10)로부터 초기에 수신한 것과 등가인지를 확인한다. 등가인 것으로 확인되면, 초기화 절차가 계속적으로 행해진다.

즉, 모빌(20)과 네트워크(10) 양자는 h(($g^{R_M} \bmod p$), h($g^{R_N} \bmod p$))를 행한다. 모빌(20)은 해시의 결과를 표시하고, 모빌 유저는, 전화 회선/지상 통신선(30)을 통해서, 해시의 디지트를 네트워크(10)에 전송한다.

네트워크(10)가 상기 디지트가 네트워크(10)에 의해 실행된 해시와 일치한다고 판정하면, 통신이 검증되고 A 키가 ($g^{R_M R_N} \bmod p$)와, 그것의 해시, 또는 그것의 일부로서 확립된다. 즉, 이렇게 하여 모빌(20)은 A키를 확립하게 되고, 네트워크(10)는 해시가 검증되는 경우 모빌(20)에만 상기 A 키를 관련시키게 된다.

다른 대안적인 예로서는, 모빌(20)과 네트워크(10) 간의 통신을 검증하기 위해 실행되는 최종 해시가 모빌(2)의 식별 번호를 포함하는 것이 있다.

앤-인-더-미들 침입자는, 네트워크(10)로서 위장하는 경우, 모빌 유저의 지수함수를 확인하기 전에 (해시를 통해) 자신이 사용하는 지수함수를 조작할 필요가 있기 때문에 버스데이 침입을 행할 수 없다. 유사하게, 침입자는, 모빌(20)로서 위장하는 경우, 해시와 관련된 네트워크의 지수함수의 값이 밝혀지기 전에 지수 함수를 조작해야만 한다.

본 발명의 실시예들중 일부에서는, 소수(p)와 생성원(g)이 모빌(20)에 사전 기억되어 있는 소정의 것이나, 그러한 경우가 아니라면, 침입자는, g와 p를 g'와 p'로 치환할 수 있으므로, 별개의 알고리즘을 효과적으로 계산할 수 있다. g와 p가 공중 전파를 통해 전송될지라도, 이들 g와 p는, 침입자에 의한 g와 p의 치환을 방지하기 위해서, 해시를 계산하기 위한 h(g,p ($g^{R_M} \bmod p$), ($g^{R_N} \bmod p$)) 의 일부로서 사용되어야 한다.

또한, 각 실시예를 전화 회선/지상 통신선(30)을 사용하는 것으로서 설명하였지만, 다른 보안 통신의 형태가 전화 회선/지상 통신선(30)을 대체할 수 있다. 예컨대, 사전에 작동되는 모빌이 전화 회선/지상 통신선을 대체할 수 있다. 대안적으로는, 전화 회선/지상 통신선 통신을, 보안성이 약간 떨어지지만, 모빌(20)과 네트워크(10) 간의 음성 채널을 통해 행할 수 있고, 그 외의 통신은 모빌(20)과 네트워크(10) 간의 제어 채널을 통해 발생할 것이다.

이와같이 설명한 본 발명은 각종 형태로 수정될 수 있음은 분명하다. 그러한 수정예는 본 발명의 사상과 범위로부터 이탈하지 않을 것이며, 그러한 수정예 전체는 첨부한 청구범위의 범위 내에 포함되리라 생각한다.

발명의 효과

본 발명에 의하면, 패스워드 프로토콜에 있어서, 통신을 행하는 파티들은 각각이 지수함수를 포함하는 계산 결과를 교환하여 키를 발생하고 있다 계산 결과의 발생에 있어서, 각 파티들은 그들의 각 지수함수에 패스워드를 추가한다. 한 파티에 의해 미리 전송된 인증 정보가 다른 파티에 의해 승인되면, 상기 다른 파티는 패스워드 프로토콜에 따라 확립된 키를 사용한다. 상기 인증 정보는 통신 보안 채널을 통해 전송된다. 각 지수함수에 패스워드를 추가함으로써, 패스워드 정보가 누출될 우려가 적어지고 상기 계산이 보다 유효하게 된다.

(57) 청구의 범위

청구항 1.

제 1 파티에서 패스워드를 사용하여 키를 확립하는 방법에 있어서,

(a) 상기 제 1 파티에서, 제 1 난수(R_M)를 발생하는 단계:

(b) ((g^{R}

^{M} + P) mod p)를 계산하여 제 1 계산 결과를 생성하는 단계로서, 여기서 P는 패스워드이고, p는 소수, g는 상기 소수(p)에 의해 발생되는 그룹의 생성원인 상기 생성 단계;

(c) 상기 소수(p), 상기 생성원(g)과 상기 제 1 계산 결과를 제 2 파티에 전송하는 단계;

(d) ((g^R_N + P) mod p)와 등가인 제 2 계산 결과를 상기 제 2 파티로부터 수신하는 단계로서, R_N은 제 2 난수인 상기 수신 단계; 및

(e) 상기 제 2 계산 결과와 상기 제 1 난수에 기초하여 키를 확립하는 단계를 포함하는 방법.

청구항 2.
제 1 항에 있어서, 상기 단계(e)는:

(e1) (P mod p)를 계산하는 단계;

(e2) ((g^R_N + P) mod p)의 상기 제 2 계산 결과로부터 (P mod p)를 감산하여 (g^R_N mod p)를 구하는 단계; 및

(e3) (g^R_N mod p)와 상기 제 1 난수에 기초하여 상기 키를 확립하는 단계를 포함하는 방법.

청구항 3.
제 1 항에 있어서, 상기 제 1 파티는 무선 통신 시스템에서의 모빌이고 상기 제 2 파티는 네트워크인 방법.

청구항 4.
제 1 항에 있어서, 상기 단계(b)는:

(f) 통신 보안 채널을 통해 인증 정보를 상기 제 2 파티에 전달하는 단계; 및

(g) 상기 제 2 파티가 상기 인증 정보를 승인하면 상기 제 2 파티로부터 상기 통신 보안 채널을 통해 상기 패스워드를 수신하는 단계를 더 포함하는 방법.

청구항 5.
제 4 항에 있어서, 상기 제 1 파티는 무선 통신 시스템에서의 모빌 유저이고 상기 제 2 파티는 네트워크이며, 상기 통신 보안 채널은 지상 통신선인 방법.

청구항 6.
제 1 파티에서 패스워드를 사용하여 키를 확립하는 방법에 있어서,

(a) 제 1 파티에서, 소수(p)와, 상기 소수에 의해 발생되는 그룹의 생성원(g), 및 제 2 파티로부터의 제 1 계산 결과를 수신하는 단계로서, 상기 제 1 계산 결과는 ((g^R_M + P) mod p)의 계산 결과이며, 여기서 P는 패스워드, R_M 은 제 1 난수인 상기 수신 단계;

(b) 제 2 난수(R_N)를 발생하는 단계;

(c) ((g^R_N + P) mod p)를 계산하여 제 2 계산 결과를 생성하는 단계;

(d) 상기 제 2 파티에 상기 제 2 계산 결과를 전송하는 단계; 및

(e) 상기 제 1 계산 결과와 상기 제 2 난수에 기초하여 키를 확립하는 단계를 포함하는 방법.

청구항 7.
제 6 항에 있어서, 상기 단계(e)는:

(e1) (P mod p)를 계산하는 단계;

(e2) (g^R_M + P) mod p)의 상기 제 2 계산 결과로부터 (P mod p)를 감산하여 ((g^R_M mod p)를 구하는 단계; 및

(e3) (g^R_M mod p)와 상기 제 2 난수에 기초하여 상기 키를 확립하는 단계를 포함하는 방법.

청구항 8.
제 6 항에 있어서, 상기 제 1 파티는 무선 통신 시스템에서의 네트워크이고 상기 제 2 파티는 모빌인 방법.

청구항 9.
제 6 항에 있어서, 상기 단계(a)의 이전에:

(f) 상기 제 2 파티로부터 통신 보안 채널을 통해 인증 정보를 수신하는 단계; 및

(g) 상기 인증정보가 승인되는 경우, 상기 제 2 파티에 상기 통신 보안 채널을 통해 상기 패스워드를 전송하는 단계를 더 포함하는 방법.

청구항 10.
제 9 항에 있어서, 상기 제 1 파티는 무선 시스템에서의 네트워크이고, 상기 제 2 파티는 모빌 유저인 방법.

청구항 11.
제 1 파티에서 키를 확립하기 위한 방법에 있어서,

(a) 상기 제 1 파티에서, 제 1 난수(R_M)를 발생하는 단계;

(b) $(g^{R_M} + P) \bmod p$)를 계산하여 제 1 계산 결과를 생성하는 단계로서, p는 소수이고, g는 상기 소수(p)에 의해 발생되는 그룹의 생성원인 상기 생성 단계;

(c) 상기 제 1 계산 결과를 제 2 파티에 전송하는 단계;

(d) $(g^{R_N} + P) \bmod p$)와 등가인 제 2 계산 결과를 상기 제 2 파티로부터 수신하는 단계로서, 여기서 R_N은 제 2 난수인 상기 수신 단계;

(e) 적어도 상기 제 1 계산 결과의 제 1 해시(hash)를 계산하는 단계;

(f) 상기 제 1 해시를 제 1 통신 보안 채널을 통해서 상기 제 2 파티에 전송하는 단계; 및

(g) 상기 제 1 난수와 상기 제 2 계산 결과에 기초하여 키를 확립하는 단계를 포함하는 방법.

청구항 12.
제 11 항에 있어서, (h) 제 2 통신 보안 채널을 통해서 상기 제 2 파티에 인증 정보를 전송하는 단계를 더 포함하고,

상기 단계(d)는, 상기 인증 정보가 상기 제 2 파티에 의해 승인되는 경우, 상기 제 2 계산 결과를 수신하는 방법.

청구항 13.
제 12 항에 있어서, 상기 단계(h)는 상기 제 1 파티에 대한 식별자를 상기 인증 정보와 함께 전송하고;

상기 단계(d)는 상기 단계(c)에 앞서 행해지거나 상기 단계(c)와 동시에 행해지는 방법.

청구항 14.
제 13 항에 있어서, 상기 단계(c)는 상기 단계(d)의 이후에 행해지는 방법.

청구항 15.
제 14 항에 있어서, 상기 단계(h)는 상기 제 1 파티에 대한 식별자를 상기 인증 정보와 함께 전송하고;

상기 단계(e)는 적어도 상기 제 1 계산 결과의 해시와 상기 제 1 파티에 대한 상기 식별자로서 상기 제 1 해시를 계산하는 방법.

청구항 16.
제 14 항에 있어서, 상기 단계(e)는 상기 제 1 및 제 2 계산 결과와 $(g^{R_N} \bmod p)^{R_M}$ 의 해시로서 상기 제 1 해시를 계산하는 방법.

청구항 17.
제 11 항에 있어서, 상기 단계(e)는 적어도 상기 제 1 및 제 2 계산 결과의 해시로서 상기 제 1 해시를 계산하는 방법.

청구항 18.
제 11 항에 있어서, 상기 제 1 파티는 무선 시스템에서의 모빌 유저이고 상기 제 2 파티는 네트워크인 방법.

청구항 19.
제 1 파티에서 키를 확립하기 위한 방법에 있어서,

(a) 제 2 파티로부터 제 1 계산 결과를 수신하는 단계로서, 상기 제 1 계산 결과는 $(g^{R_M} \bmod p)$의 계산 결과이며, 여기서 R_M 은 제 1 난수이고, p는 소수이고, g는 상기 소수(p)에 발생되는 그룹의 생성원인 상기 수신 단계;

(b) 제 2 난수(R_N)를 발생하는 단계;

(C) $(g^{R_N} \bmod p)$를 계산하여 제 2 계산 결과를 생성하는 단계;

(d) 상기 제 2 계산 결과를 상기 제 2 파티에 전송하는 단계;

(e) 적어도 상기 제 1 계산 결과의 제 1 해시를 계산하는 단계;

(f) 제 1 통신 보안 채널을 통해 상기 제 2 파티로부터 제 2 해시를 수신하는 단계;

(g) 상기 제 1 및 제 2 해시에 기초하여 상기 제 2 파티를 검증하는 단계; 및

(h) 상기 제 2 파티가 검증되는 경우 상기 제 2 난수와 상기 제 1 계산 결과에 기초하여 키를 확립하는 단계를 포함하는 방법.

청구항 20.
제 19 항에 있어서, (i) 제 2 통신 보안 채널을 통해서 상기 제 2 파티로부터 인증 정보를 수신하는 단계를 더 포함하고,

상기 단계(d)는 상기 인증 정보가 승인되는 경우 상기 제 2 파티에 상기 제 2 계산 결과를 전송하는 방법.

청구항 21.
제 20 항에 있어서, 상기 단계(i)는 상기 제 2 파티에 대한 식별자를 상기 인증 정보와 함께 수신하고,

상기 단계(d)는 상기 단계(a)에 앞서 행해지거나 상기 단계(a)와 동시에 행해지는 방법.

청구항 22.
제 21 항에 있어서, 상기 단계(a)는 상기 단계(a)의 이후에 행해지는 방법.

청구항 23.
제 22 항에 있어서, 상기 단계(i)는 상기 제 2 파티에 대한 식별자를 상기 인증 정보와 함께 수신하고,

상기 단계(e)는 적어도 상기 제 1 계산 결과와 상기 제 2 파티에 대한 식별자의 해시로서 상기 제 1 해시를 계산하는 방법.

청구항 24.
제 22 항에 있어서, 상기 단계(e)는 상기 제 1 및 제 2 계산 결과와 $(g\hat{}R_M \mod p)\hat{}R_N$ 의 해시로서 상기 제 1 해시를 계산하는 방법.

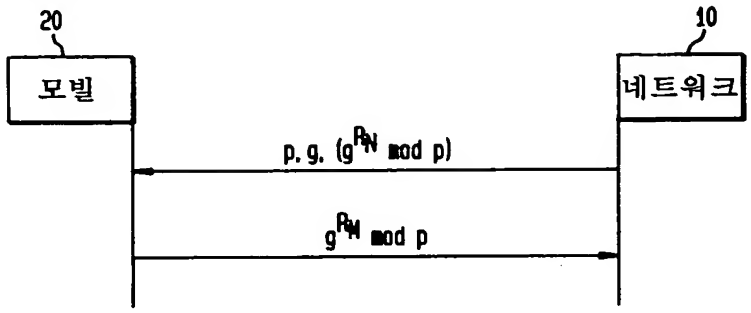
청구항 25.
제 19 항에 있어서, 상기 단계(e)는 적어도 상기 제 1 및 제 2 계산 결과의 해시로서 상기 제 1 해시를 계산하는 방법.

청구항 26.
제 19 항에 있어서, 상기 제 1 파티는 무선 시스템에서의 네트워크이고 상기 제 2 파티는 모빌 유저인 방법.

도면

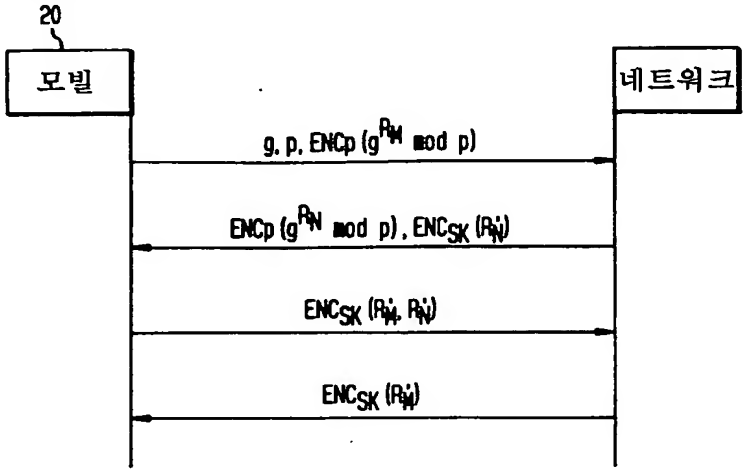
도면 1

(종래기술)

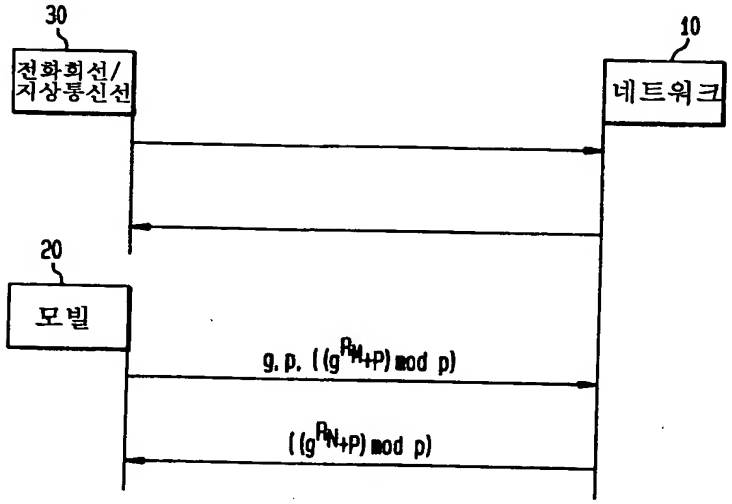


도면 2

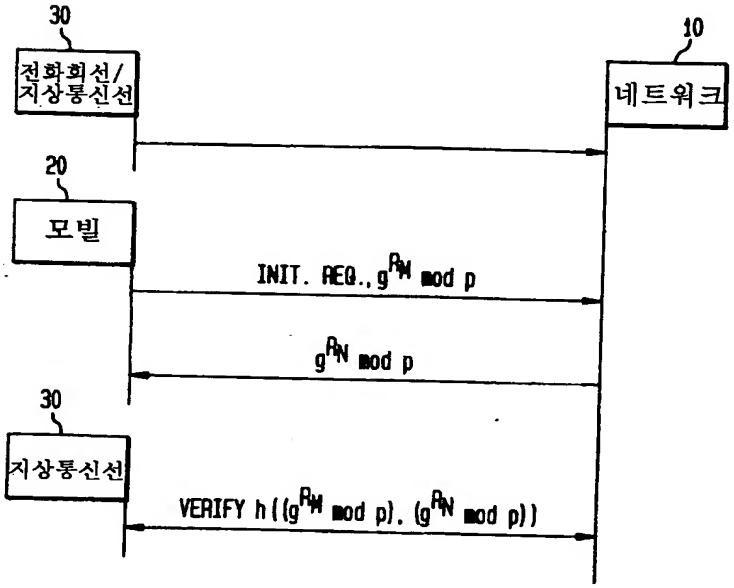
(종래기술)



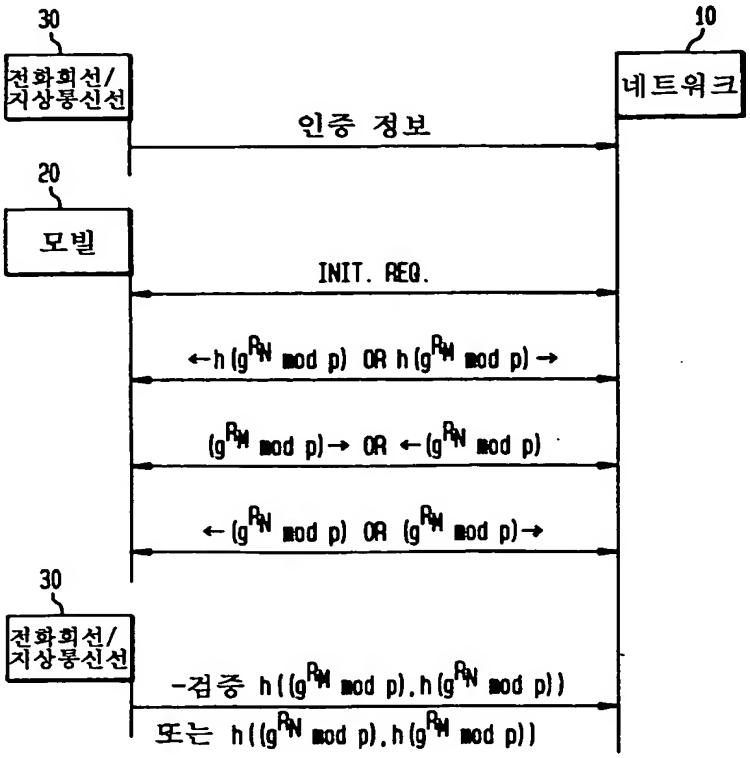
도면 3


30
전화회선/
지상통신선
10
네트워크
20
모빌
g, p, ((g^RM+P) mod p)
((g^RN+P) mod p)

도면 4


30
전화회선/
지상통신선
10
네트워크
20
모빌
INIT. REQ., g^RM mod p
g^RN mod p
30
지상통신선
VERIFY h((g^RM mod p), (g^RN mod p))

도면 5


30
전화회선/
지상통신선
10
네트워크
인증 정보
20
모빌
INIT. REQ.
←h(g^RN mod p) OR h(g^RM mod p)→
(g^RM mod p)→ OR ←(g^RN mod p)
←(g^RN mod p) OR (g^RM mod p)→
30
전화회선/
지상통신선
-검증 h((g^RM mod p),h(g^RN mod p))
또는 h((g^RN mod p),h(g^RM mod p))